

ORDER

U.S. DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION
WESTERN-PACIFIC REGION

WP 1600.27

10/19/90

SUBJ: DATA GENERAL COMPUTER PASSWORD CONTROL

1. PURPOSE. This order establishes procedures for password control for users on the Data General (DG) computers.
2. DISTRIBUTION. This order is distributed to all employees in the Regional Headquarters and to a maximum level in field offices and facilities in Western-Pacific Region.
3. BACKGROUND. In order to meet security standards of FAA Order 1600.54B, FAA Automated Information Systems Handbook, and to better protect the integrity of application systems on the regional host computers (DG MV 15000's), the password on each DG user ID must be changed every 90 days. Password control software has been installed and is now being implemented to assist in compliance with this policy.
4. PROCEDURES. The following are instructions for the use of this software:

a. When the user ID is established, an initial password is assigned that must be changed when the user logs on the first time. The message will read as follows:

"Your password is only valid for this session and must be changed.

Please choose a new password or enter 'new line' for a system-generated password.

Please enter the password again for verification."

Enter your choice of password. If you do not choose a password, enter 'new line' and the system will assign the password.

The password (assigned or selected) shall not be identifiable to the individual (e.g., social security number, birth date, etc.) and SHALL NOT be written down. The protection of the passwords shall be sufficient to ensure that they are not compromised through carelessness or negligence. They shall not be based upon information that can be derived by the knowledge of the authorized user.

Distribution: A-X-8; A-FOF-0 (MAX)

Initiated By: AWP-40

Users shall assure that passwords or other terminal access data are not left on discarded printouts, discarded listings, or unattended video display terminals.

Passwords shall be managed by the Data General System Manager.

b. The password (assigned or selected) will now be in effect for 90 days.

c. On the day the password expires or the first logon after that date, the user will be prompted for a new password during the logon sequence. The logon sequence will not be completed until a valid password has been selected.

d. The password selected must not repeat any five previous passwords. A message will appear if this happens and a prompt for a different password will be given.

e. The password must be 6 to 15 characters in length. (Spaces and special characters can be used.)

f. There are several words reserved in password selection and if one is used, a message will appear and again a prompt for a different password will be given.

After completing the password selection, the system will continue as usual.

g. The user IDs that were established prior to installation of this software are being converted to run under the new software. Current passwords now in effect will remain so for 90 days. At that time, the message advising that the password has expired will appear and appropriate action must be taken following the above instructions.

5. MISUSE OF PRIVILEGES. FAA employees who are authorized access to an FAA computer system who knowingly misuse or abuse a system will be subject to disciplinary action under the provisions of Order 3750.4, Conduct and Discipline Handbook, as well as any criminal penalties which may result from data alteration, system misuse, or diversion of system resources for personal gain or profit.

6. SECURITY INCIDENTS. All security incidents will be reported to the respective Automated Information Systems Security Officer (AISSO). Incidents of system misuse or abuse, or other use of Automated Information Systems (AIS) contrary to law or FAA regulations, shall be reported to the Civil Aviation Security Division, Investigations and Internal Security Branch, AWP-710, for arranging for investigation when appropriate.



Richard G. Cambra
Manager, Financial & Management
Resources Division